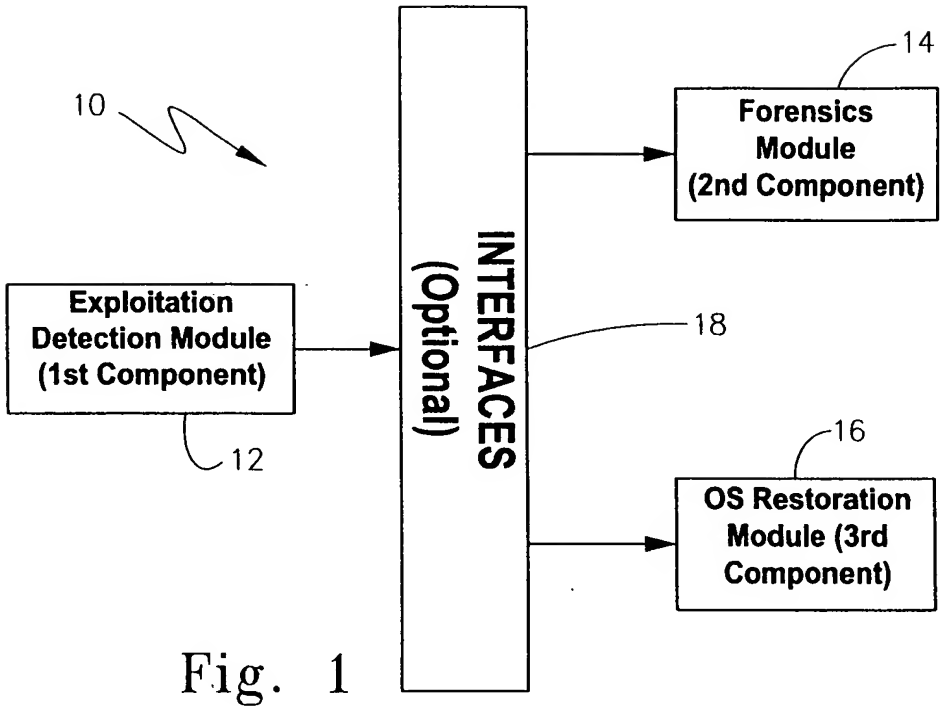

Fig. 1

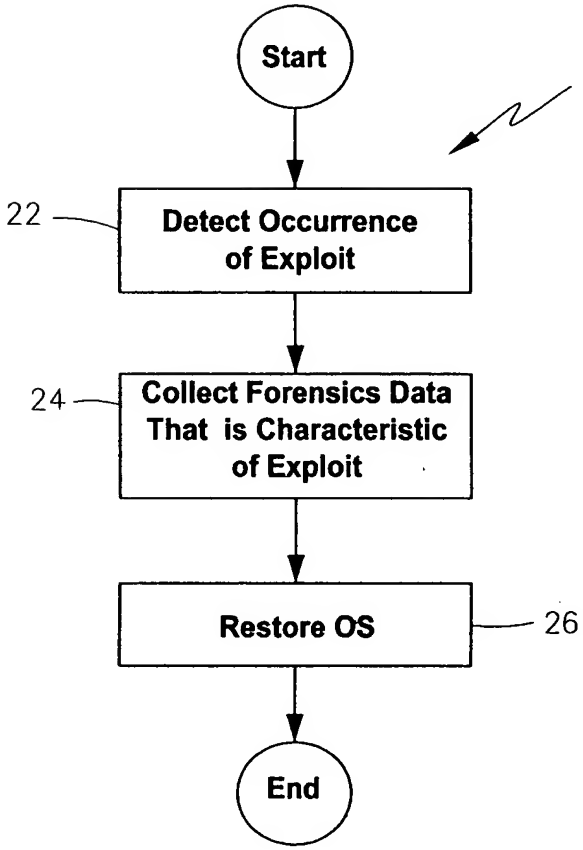

Fig. 2

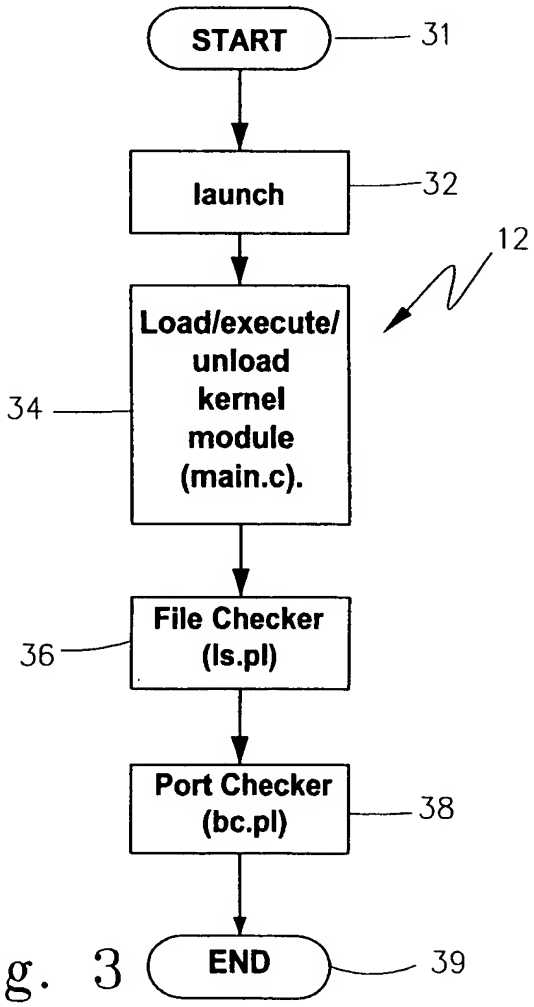

Fig. 3

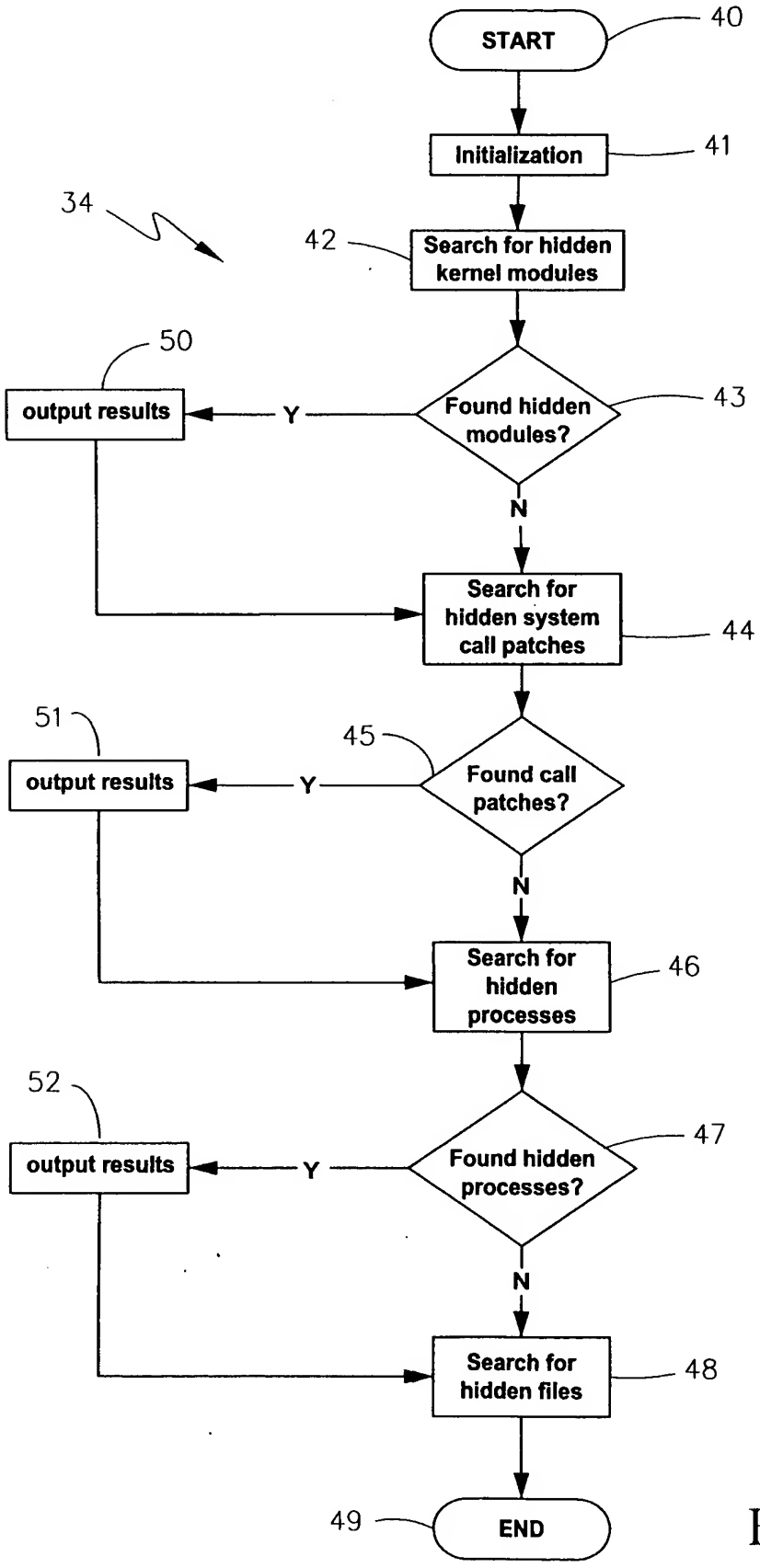
START
40
Initialization
41
34
42
Search for hidden kernel modules
50
output results
Y
Found hidden modules?
43
N
Search for hidden system call patches
44
51
output results
Y
45
Found call patches?
N
Search for hidden processes
46
52
output results
Y
Found hidden processes?
47
N
Search for hidden files
48
49
END

Fig.4

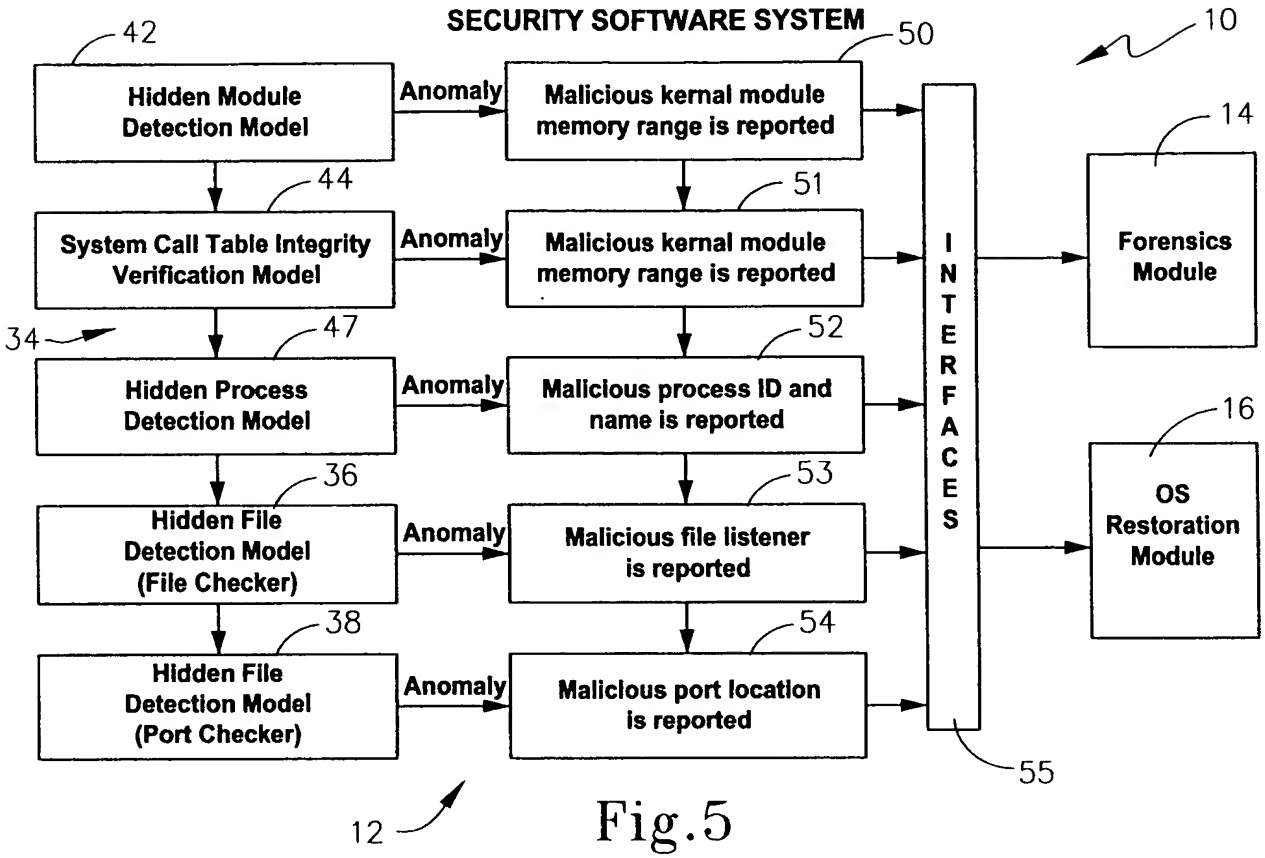

Fig.5

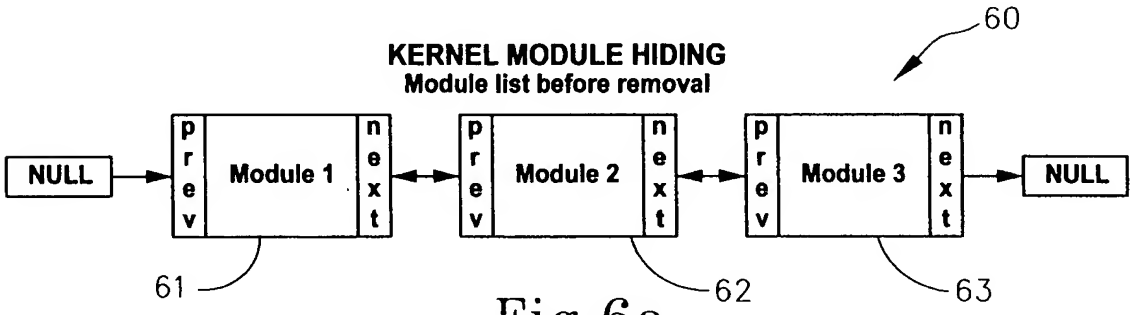

Fig.6a

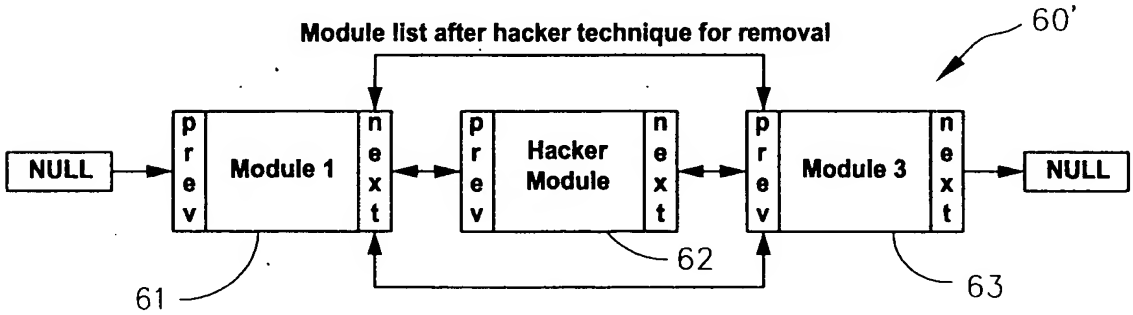

Fig.6b

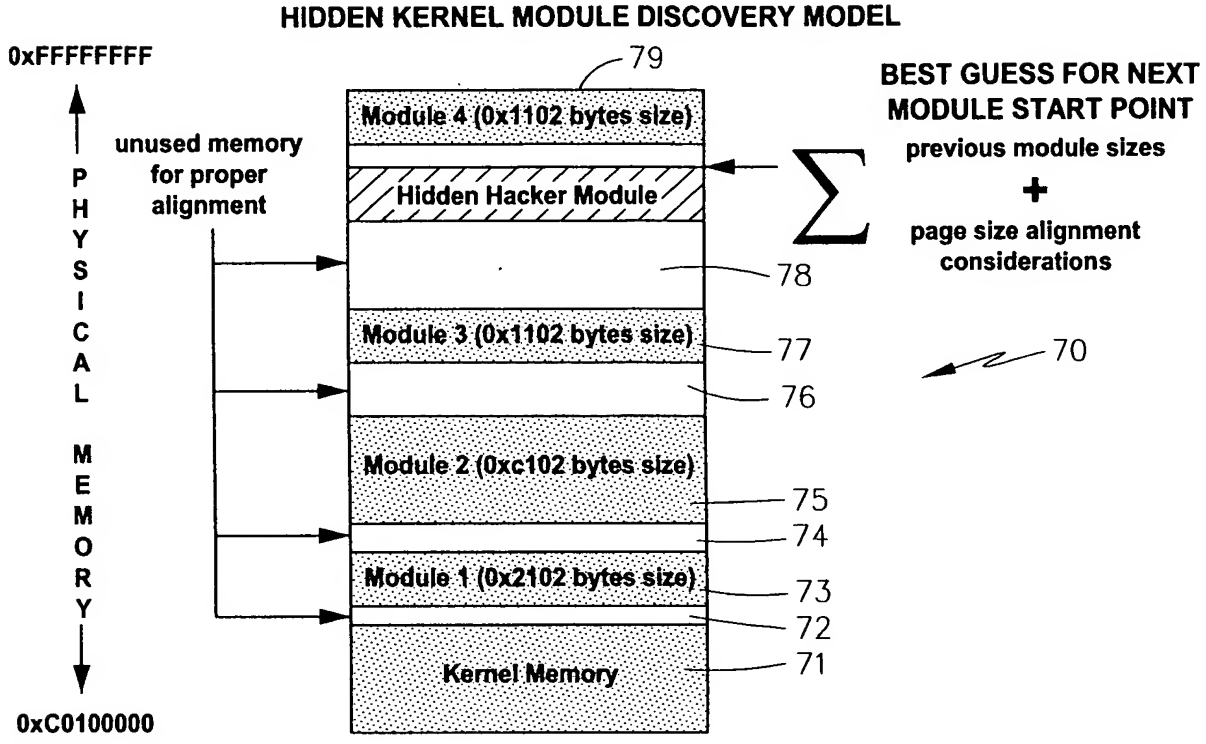
HIDDEN KERNEL MODULE DISCOVERY MODEL
0xFFFFFFFF
PHYSICAL MEMORY
0xC0100000
unused memory for proper alignment
79
Module 4 (0x1102 bytes size)
Hidden Hacker Module
78
Module 3 (0x1102 bytes size)
77
76
Module 2 (0xc102 bytes size)
75
74
Module 1 (0x2102 bytes size)
73
72
Kernel Memory
71
BEST GUESS FOR NEXT MODULE START POINT
previous module sizes
+
page size alignment considerations
70

Fig.7

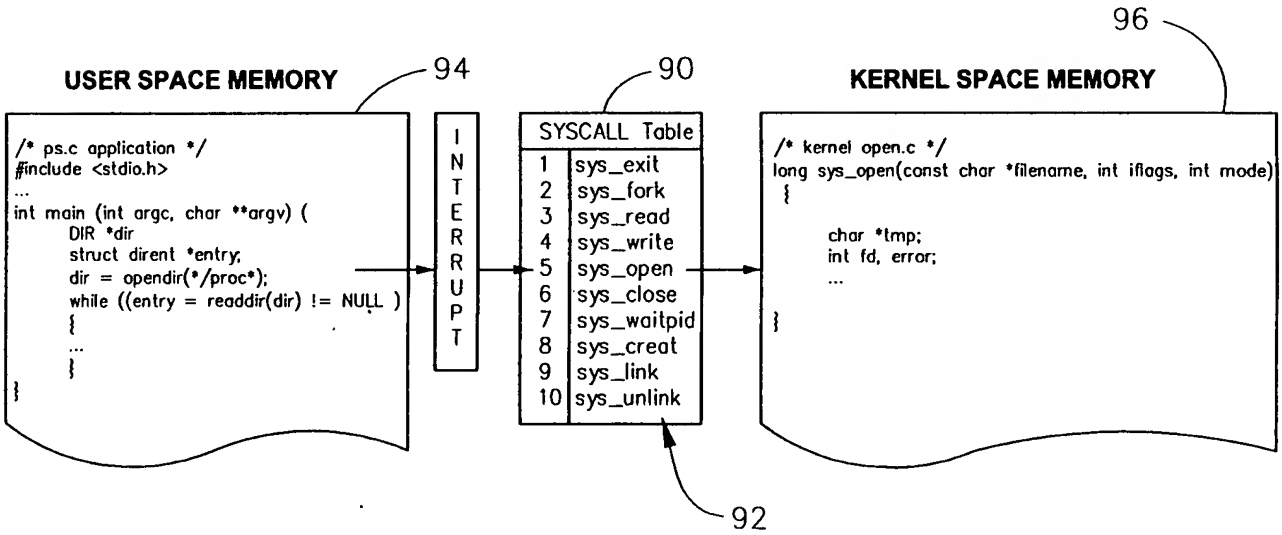
USER SPACE MEMORY
94
/* ps.c application */
#include <stdio.h>
...
int main (int argc, char **argv) {
DIR *dir
struct dirent *entry;
dir = opendir("/proc");
while ((entry = readdir(dir) != NULL)
{
...
}
}
INTERRUPT
90
SYSCALL Table
1 sys_exit
2 sys_fork
3 sys_read
4 sys_write
5 sys_open
6 sys_close
7 sys_waitpid
8 sys_creat
9 sys_link
10 sys_unlink
92
96
KERNEL SPACE MEMORY
/* kernel open.c */
long sys_open(const char *filename, int iflags, int mode)
{
char *tmp;
int fd, error;
...
}

Fig.9

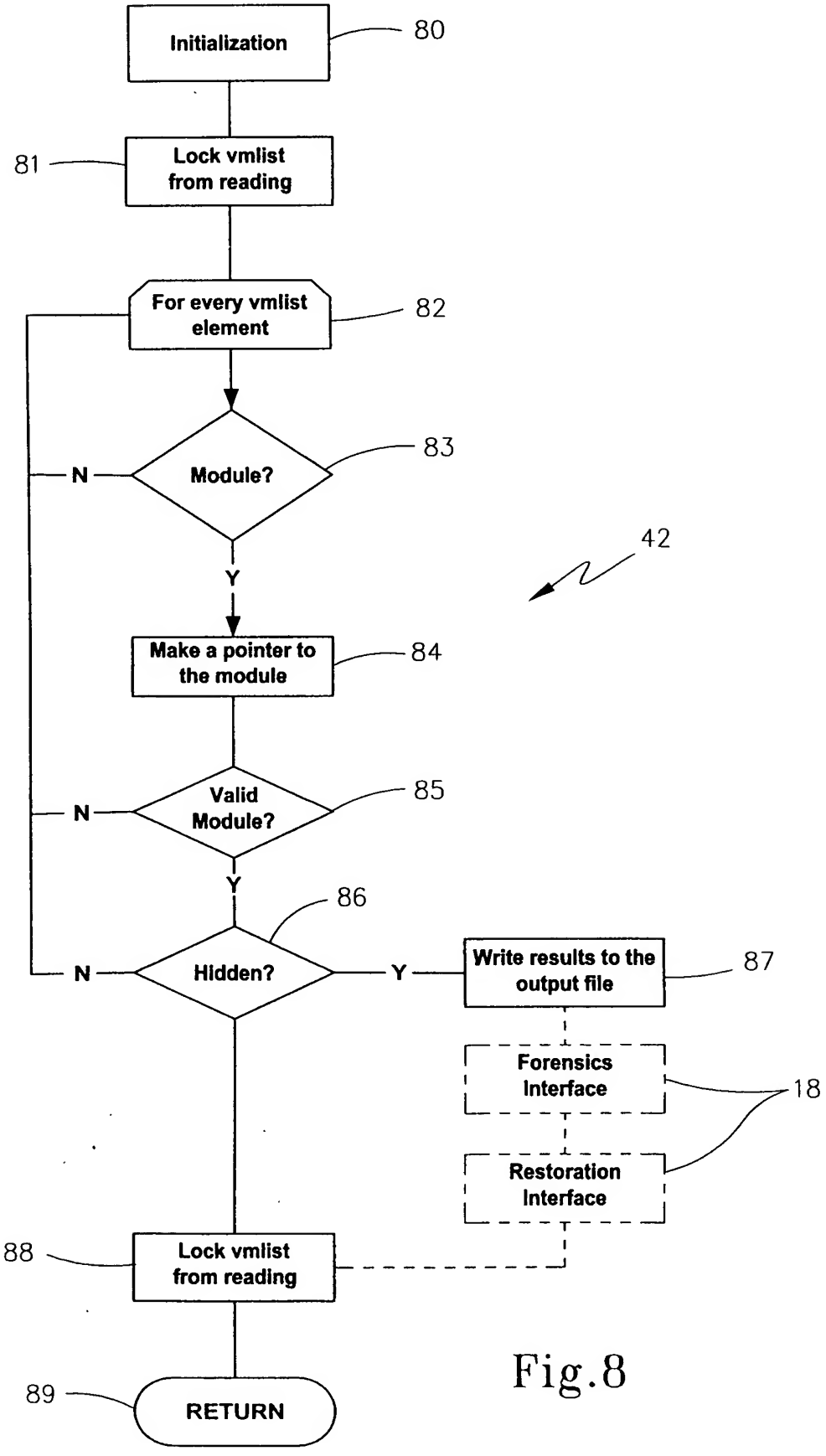
Initialization
80
Lock vmlist from reading
81
For every vmlist element
82
Module?
83
N
Y
42
Make a pointer to the module
84
Valid Module?
85
N
Y
86
Hidden?
N
Y
Write results to the output file
87
Forensics Interface
18
Restoration Interface
Lock vmlist from reading
88
RETURN
89

Fig.8

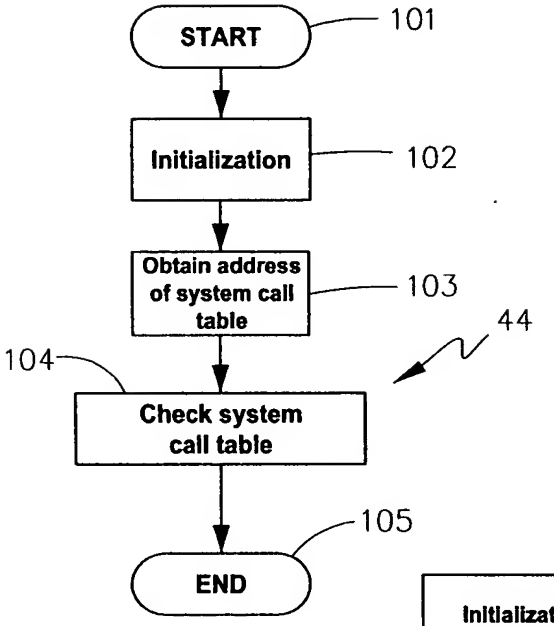

Fig.10a

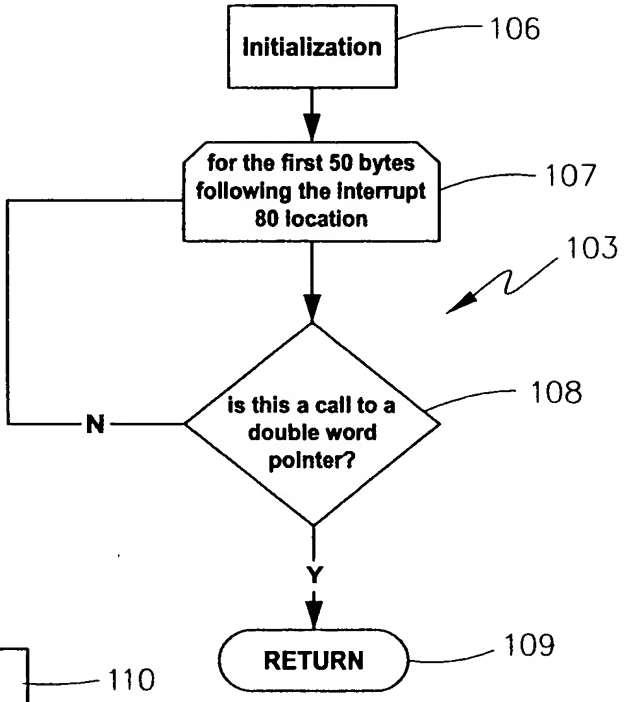

Fig.10b

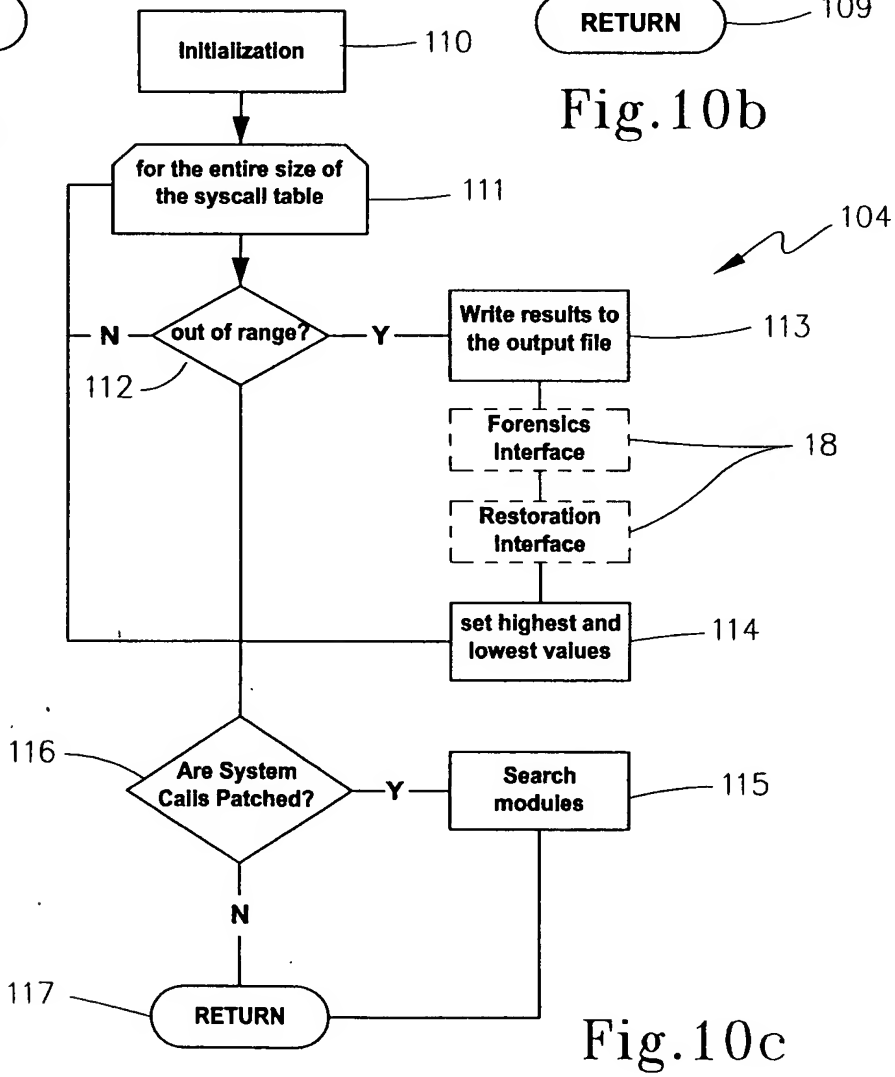

Fig.10c

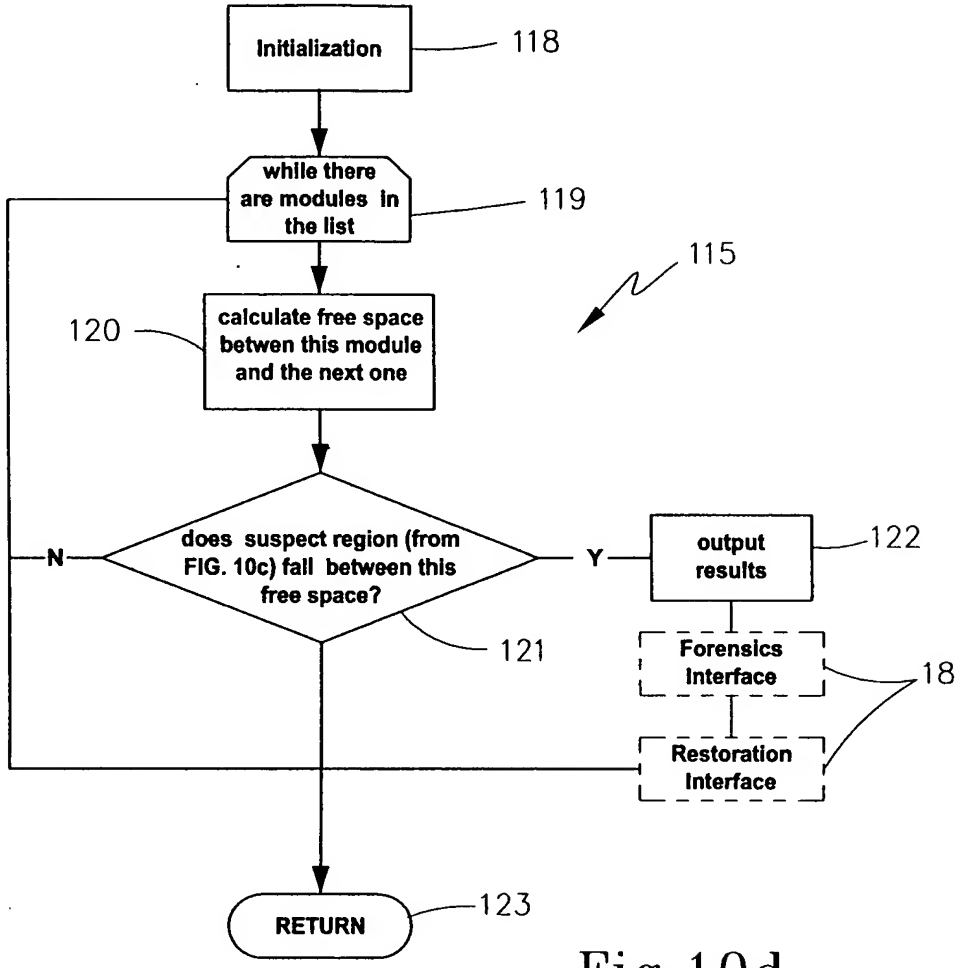

Fig.10d

IDENTIFIED SYSCALL ANOMALIES CAUSE BY ADORE v0.42

syscall [2]	fork	FAILED	0xf8aca650
syscall [4]	write	FAILED	0xf8aca7e8
syscall [5]	open	FAILED	0xf8acb184
syscall [6]	close	FAILED	0xf8aca898
syscall [18]	oldstat	FAILED	0xf8acabe4
syscall [37]	kill	FAILED	0xf8aca710
syscall [39]	mkdir	FAILED	0xf8aca9a0
syscall [84]	oldlstat	FAILED	0xf8acacd0
syscall [106]	stat	FAILED	0xf8acadbc
syscall [107]	lstat	FAILED	0xf8acae94
syscall [120]	clone	FAILED	0xf8aca6b0
syscall [141]	getdents	FAILED	0xf8aca368
syscall [195]	stat64	FAILED	0xf8acaf80
syscall [196]	lstat64	FAILED	0xf8acb080
syscall [220]	getdents64	FAILED	0xf8aca4dc

125
Highest
127
Lowest

```
analyze_memory ( highest, lowest) {

    if the range falls between two
    valid kernel modules then flag
    the entire memory range in
    between the two as a malicous
    kernel module.

}
```

Fig.11

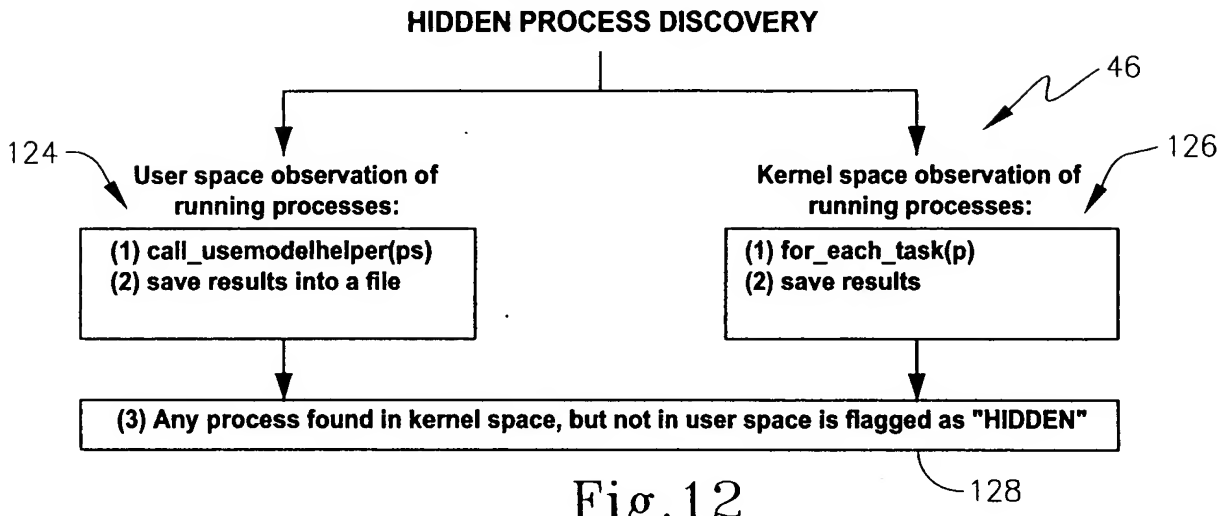

Fig.12

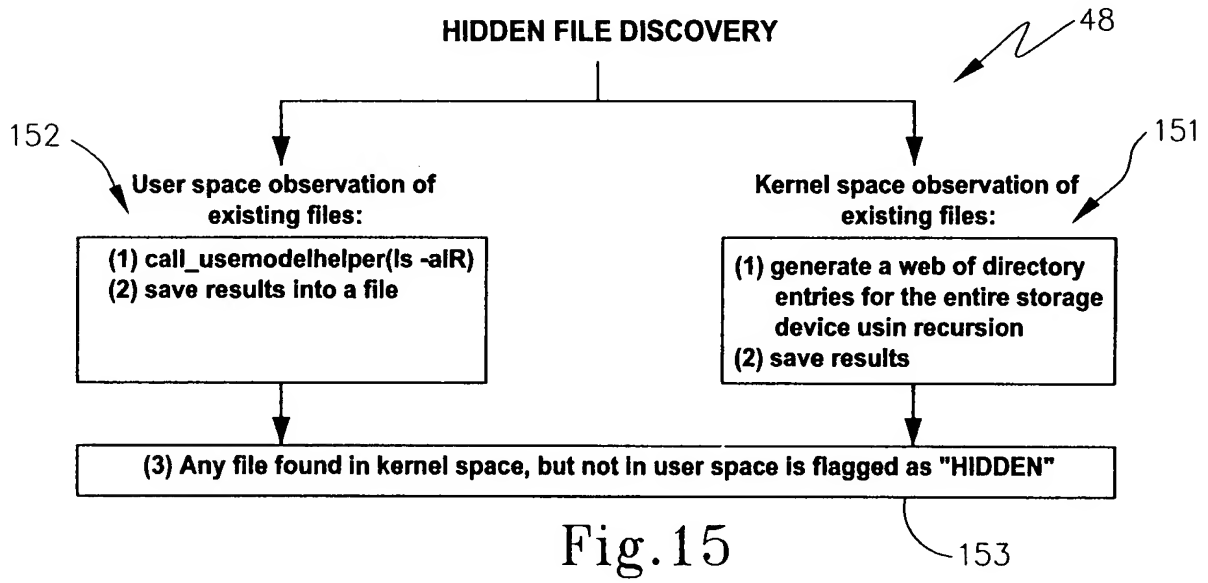

Fig.15

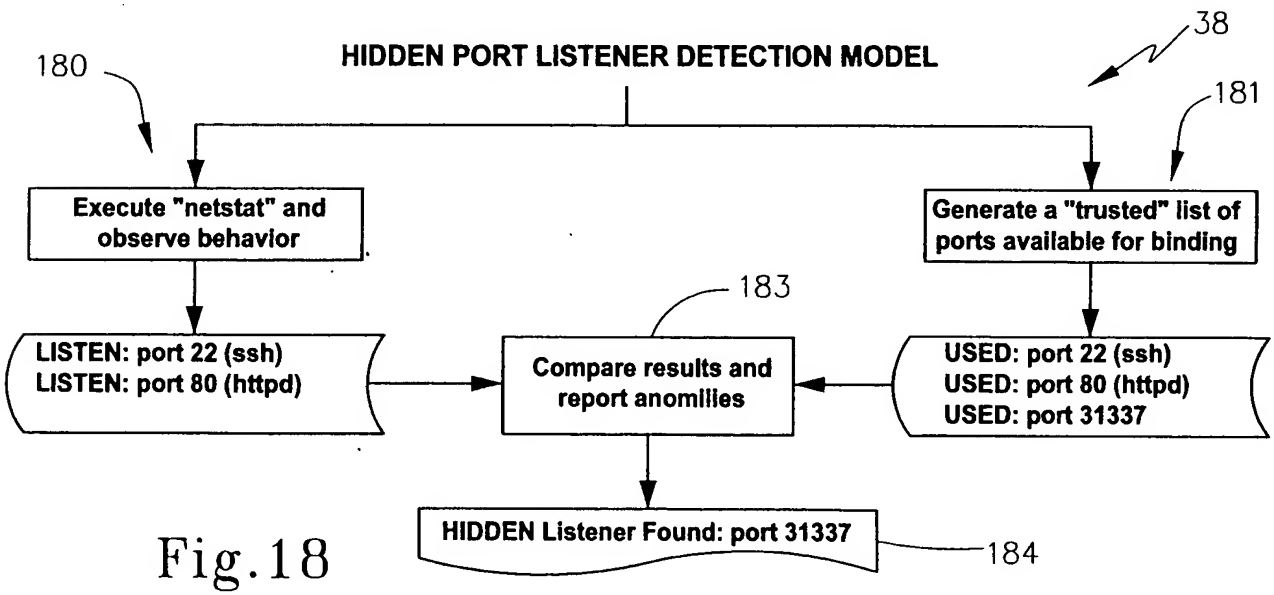

Fig.18

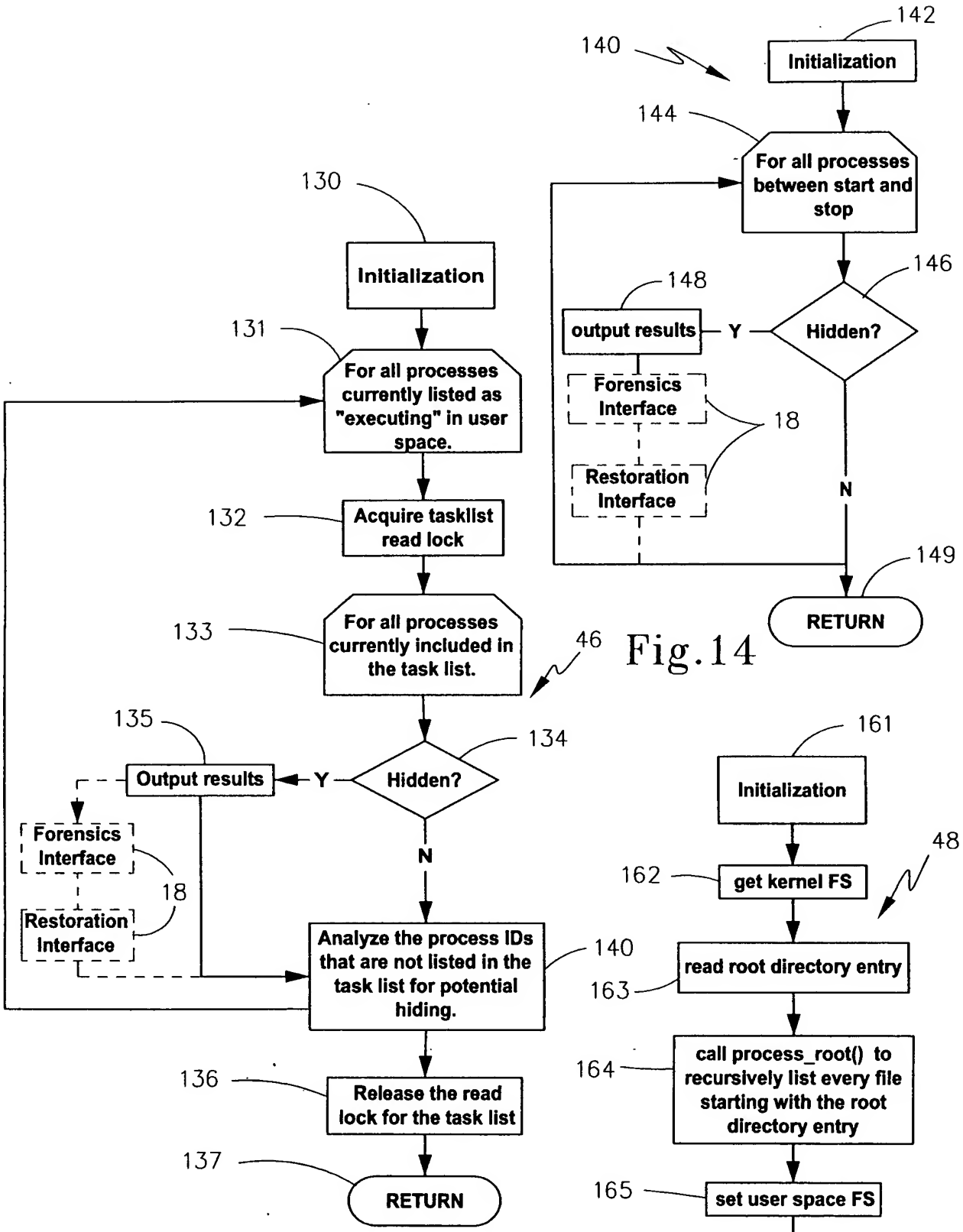

Fig.13

Fig.14

Fig.16

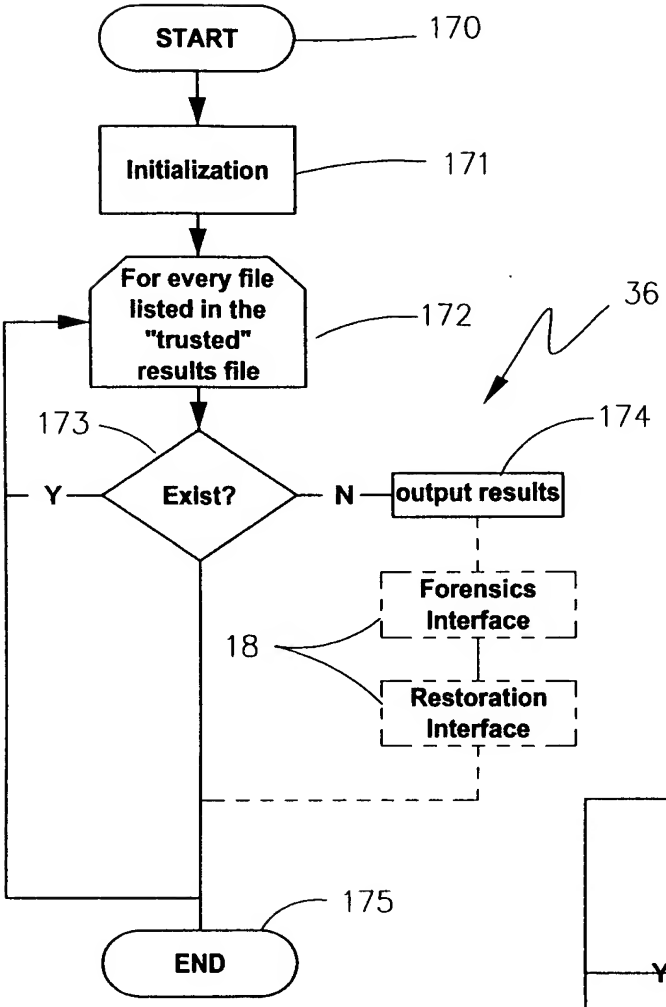
START
170
Initialization
171
For every file listed in the "trusted" results file
172
36
173
Exist?
Y
N
output results
174
Forensics Interface
18
Restoration Interface
175
END

Fig. 17

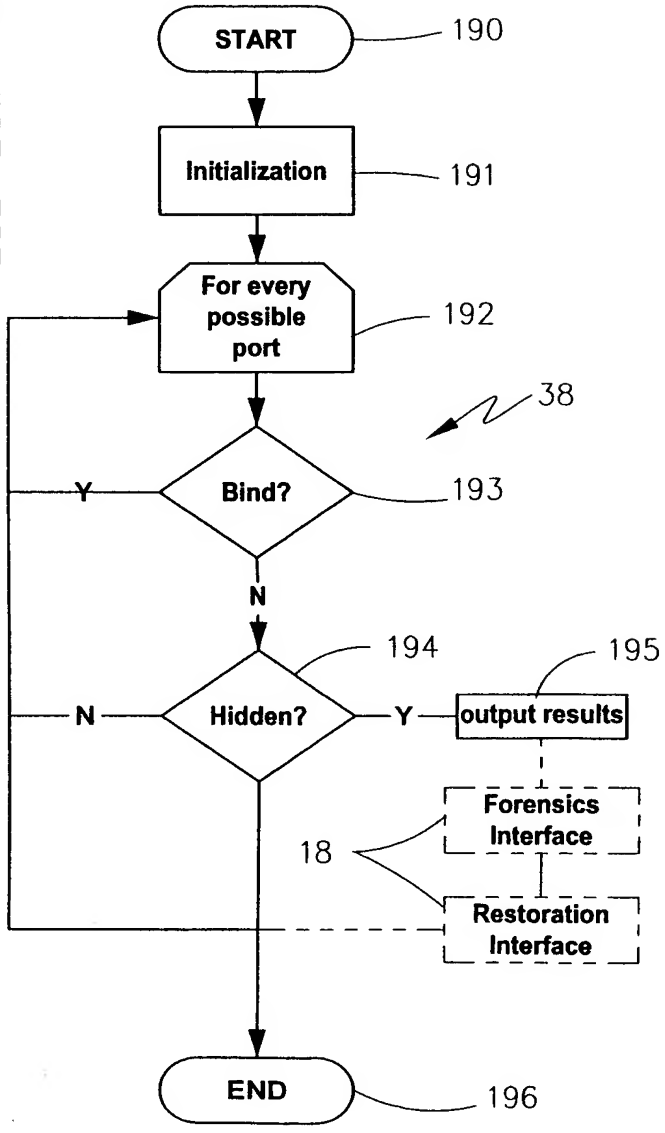
START
190
Initialization
191
For every possible port
192
38
Bind?
Y
193
N
194
Hidden?
N
Y
195
output results
Forensics Interface
18
Restoration Interface
END
196

FIG. 19

```
Script started on Sat Aug  9 15:42:00 2003
[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator- this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

----------------------[ SUMMARY ]----------------------

NO hidden modules were found.
NO system call table modifications were found.
NO hidden processes were found.
WARNING: File size is 60133 (should be 58885): /var/log/sa/sa09
WARNING: File size is 1010871 (should be 1010003) : /var/log/cron
WARNING: File size is 597700 (should be 597264): /var/log/maillog
NO hidden files were found.
NO hidden TCP port listeners were found.
[root@localhost interrogator)# exit
Script done on Sat Aug 9 16:01:52 2003
```

200

Fig.20a

```
(root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator- this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

----------------------[ SUMMARY ]----------------------
NO hidden modules were found.
NO system call table modifications were found

WARNING: process id 13745 hidden or just exited (tb)
Launch Path: /root/code/interrogator/de.rojansans/tb
FOUND 1 Hidden process listing

HIDDEN file found: /tmp/hideme
WARNING: File size is 62629 (should be 61381): /var/log/sa/sa09
WARNING: File size is 1013693 (should be 1012816): /var/log/cron
WARMING: File size is 599450 (should be 599012): /var/log/maillog

HIDDEN TCP Port Listener found: port 2222
(root@localhost interrogator]# exit
```

202

Fig.20b

```
[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator. . .this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

-------------------------[ SUMMARY ]-------------------------
WARNING suspect module found: f8a0f000 8000 bytes (adore)
Image stored at /tmp/interrogator/adore.o
FOUND 1 HIDDEN module loaded

WARNING: Deviations found in the sys_call_table
syscall[2]      FAILED  0xf8a0f650      fork
syscall[4]      FAILED  0xf8a0f7e8      write
syscall[5]      FAILED  0xf8a10184      open
syscall[6]      FAILED  0xf8a0f898      close
syscall[18]     FAILED  0xf8a0fbe4      oldstat
syscall[37]     FAILED  0xf8a0f710      kill
syscall[39]     FAILED  0xf8a0f9a0      mkdir
syscall[84]     FAILED  0xf8a0fcd0      oldlstat
syscall[106]    FAILED  0xf8a0fdbc      stat
syscall[107]    FAILED  0xf8a0fe94      lstat
syscall[120]    FAILED  0xf8a0f6b0      clone
syscall[141]    FAILED  0xf8a0f368      getdents
syscall[195]    FAILED  0xf8a0ff80      stat64
syscall[196]    FAILED  0xf8a10080      lstat64
syscall[220]    FAILED  0xf8a0f4dc      getdents64
Suspect module located (0xf89da6d8 - 0xf8a12000)
FOUND 15 Modified syscall table functions

WARNING: Found process id 836 removed from the task_queue.
Launch Path: /root/code/interrogator/demo/trojans/test
WARNING: process id 13745 hidden or just exited (tb)
Launch Path: /root/code/interrogator/demo/trojans/tb
FOUND 2 Hidden process listings

HIDDEN File found:  /mp/hideme
WARNING: File size is 2336990 (should be 2335392): /var/log/messages

HIDDEN TCP Port Listener found: port 111
HIDDEN TCP Port Listener found: port 139
HIDDEN TCP Port Listener found: port 2222
HIDDEN TCP Port Listener found: port 6000
HIDDEN TCP Port Listener found: port 32768
HIDDEN TCP Port Listener found: port 32769

[root@localhost interrogator]# exit
```

204

Fig.20c

```
[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator... this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

-------------------------[ SUMMARY ]-------------------------
WARNING suspect module found: f8a10000 184700 bytes (homegrown)
FOUND 1 HIDDEN module loaded

WARNING: Deviations found in the sys_call_table
syscall[3]      FAILED  0xf8a11494      read
syscall[5]      FAILED  0xf8a11020      open
syscall[11]     FAILED  0xf8a10ebc      execve
syscall[13]     FAILED  0xf8a118a0      time
syscall[78]     FAILED  0xf8a1183c      gettimeofday
syscall[141]    FAILED  0xf8a11544      getdents
syscall[220]    FAILED  0xf8a116c0      getdents64

Suspect module located (0xf89db6d8 - 0xf8a3f000)
FOUND 7 Modified syscall table functions

WARNING: process id 1584 hidden or just exited (tb)
Launch Path: /root/code/interrogator/demo/trojans/tb
FOUND 1 Hidden process listing

HIDDEN File found: /tmp/hideme
WARNING: File size is 1021523 (should be 1020648): /var/log/cron
WARNING: File size is 603820 (should be 603384): /var/log/maillog

HIDDEN TCP Port Listener found: port 2222
[root@localhost interrogator]# exit
```

206

Fig.20d